2019

Cyber Security Awareness Among College Students

Abbas Moallem
San Jose State University, abbas.moallem@sjsu.edu

Recommended Citation

Abbas Moallem. "Cyber Security Awareness Among College Students" *Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing* (2019): 79-87. https://doi.org/10.1007/978-3-319-94782-2_8

Cyber Security Awareness Among College Students

Abbas Moallem

UX Experts, LLC, Cupertino, CA 95014
San Jose State University, San Jose, California, USA
Abbas.moallem@sjsu.edu

Abstract. This study reports the early results of a study aimed to investigate student awareness and attitudes toward cyber security and the resulting risks in the most advanced technology environment: the Silicon Valley in California, USA. The composition of students in Silicon Valley is very ethnically diverse. The objective was to see how much the students in such a tech-savvy environment are aware of cyber-attacks and how they protect themselves against them. The early statistical analysis suggested that college students, despite their belief that they are observed when using the Internet and that their data is not secure even on university systems, are not very aware of how to protect their data. Also, it appears that educational institutions do not have an active approach to improve awareness among college students to increase their knowledge on these issues and how to protect themselves from potential cyber-attacks, such as identity theft or ransomware.

Keywords: Cyber Security Awareness, Trust, Privacy, Cyber Security User Behavior, Two-factor authentication

1 Introduction

In September 2017, Equifax, one of three major credit-reporting agencies in the United States, revealed that highly sensitive personal and financial information for about 143 million American consumers was compromised in a cyber security breach that began in late spring that year. [1]

Every day, cyber-criminals exploit a variety of threat vectors, including email, network traffic, user behavior, and application traffic to insert ransomware. [2] For example, cyber-criminals use e-mail wiretapping to create an HTML e-mail that, each time it's read, can send back a copy of the email's contents to the originator. This gives the author of the e-mail an opportunity to see whom the email was subsequently forwarded to and any forwarded messages.

Today technology facilitates communication and one can chat with someone in the next room or another country with ease, via a variety of technologies. This ease of communication also prepared the ground for Cyber stalking, which has been defined as the use of technology, particularly the Internet, to harass someone. Common characteristics include false accusations, monitoring, threats, identity theft, and data de-

struction or manipulation. Cyber stalking also includes exploitation of minors, be it sexual or otherwise. Approximately 4.9% of students had perpetrated cyber stalking. [3]

These cases show to what extent any individual using the Internet and computers is vulnerable to cyber-attacks, which affect not just businesses or organizations but also any one individual.

Users' understanding of risks and how to protect themselves from cyber-attacks is therefore fundamental in modern life. After all, from banking and e-commerce to pictures of private information and documents, so much can be compromised. Also, all information breaches of companies detaining user information can be easily subject users to identity theft. What users can do to protect themselves and what actions they should take depend on their awareness and knowledge of the risks. The FTC's Consumer Sentinel Network, which collects data about consumer complaints including identity theft, found that 18% of people who experienced identity theft in 2014 were between the ages of 20 and 29. [4,5]

Several studies have been conducted in recent years to measure the level of awareness among college students concerning information security issues. Slusky and Partow-Navid [6] surveyed students at the College of Business and Economics at California State University, Los Angeles. The results suggest that the major problem with security awareness is not due to a lack of security knowledge, but rather in the way that students apply that knowledge in real-world situations. Simply put, compliance with information security knowledge is lower than the understanding or awareness of it.

Another study by Samaher Al-Janabi and Ibrahim Al-Shourbaji [7] analyzed cyber security awareness among academic staff, researchers, undergraduate students, and employees in the education sector in the Middle East. The results reveal that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in day-to-day work.

In a study [8] aimed to analyze cyber security awareness among college students in Tamil Nadu (a state in India) about various security threats, 500 students in five major cities took the online survey. The result showed that more than 70% of students were more conscious about basic virus attacks and using antivirus software (updating frequently) or Linux platforms to safeguard their system from virus attacks. The remaining students were not using any antivirus and were the victims for virus attacks. 11% of them were using antivirus but they were not updating their antivirus software. More than 97% of them didn't know the source of the virus.

To understand the awareness of risks related to social networking sites (SNSs), a study [9] was conducted among Malaysian undergraduate students of which 295 took part. This study reported that more than one-third of participants had fallen victim to SNS scams.

The objective of the current study is to investigate student awareness and attitudes toward cyber security and the resulting risks among the most advanced technology environment: California's Silicon Valley. The composition of students in Silicon Valley is very ethnically diverse. According to the San Jose State University website, 51% of student are male and 49% females. The diversity of students by ethnicity is 41% Asian, 26% Hispanic, 19% white and 14% other. The average age of undergraduate students in Fall 2017 was 22.6 [10]. Our objective was to see how much the students in such a tech-savvy environment were aware of cyber-attacks and how they protect themselves against cyber-attacks.

2 Method

The study was designed to collect quantitative data with an online survey. The survey has been administered to students of two California State Universities in Silicon Valley in 2017 and the first quarter of 2018 using a Qualtrics survey application. The survey was administered to students enrolled in three different courses (Human-Computer Interaction, Human Factors/Ergonomics, and Cyber security) before starting each course. The result was shared for each group of students at one session on cyber security.

The study includes the following ten questions:

- Do you consider yourself knowledgeable about the concept of cyber security?
- When using the computer system and Internet, what do you consider being private information?
- On a scale of one to ten (one being the least secure and ten being the most secure), rank how secure you think your communications are on each of the following platforms.
- Do you use a harder-to-guess password to access your bank account than to access your social networking accounts?
- Do you know what Two-Factor Authentication (2FA) is and do you use it?
- Have you ever rejected a mobile app request for accessing your contacts, camera or location?
- Do you ever reject app permission?
- Do you have reason to believe that you are being observed online without your consent?
- Do you think that your data on the university system is secure?
- Do you think your communication through the Learning Management System is secure?

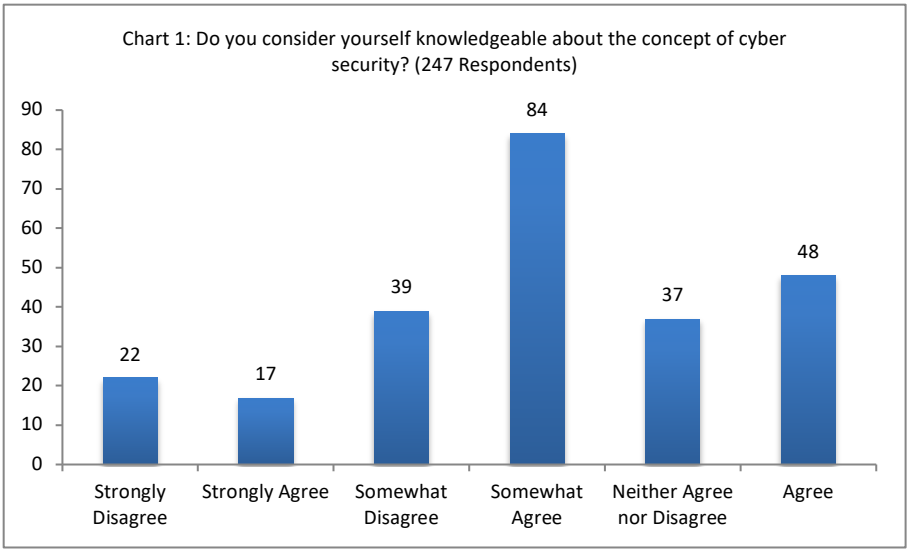
247 students have completed the survey online survey. No demographic data beside gender and age range were collected. We did not collect any personal identifying data about respondents. 34% (85) of respondents are female and 65% (162) are males. 56% (139) of the respondents are 18-24 years old, 41%(101) are 25-34 years old, and 7% are over 35 years old. Thus, overall the respondents are very young, as expected for college students. Around 70% are undergraduates and graduate students enrolled in software engineering programs, and 30% are in human factors.

3 Results

The results of the study from the 247 surveyed students are summarized below.

Knowledge of Cyber Security

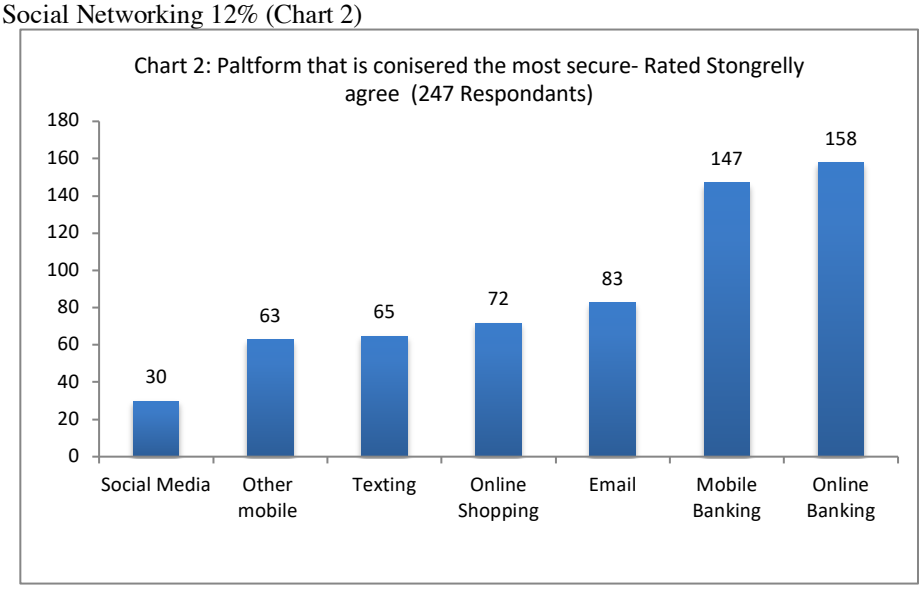
In response to the question regarding their knowledge of the concept of cyber security, only 26% agree that they are knowledgeable (agree or strongly agree), 49% believe they have average knowledge (somewhat agree or neither agree nor disagree), and 24% reported they are not knowledgeable (somewhat disagree or strongly disagree). The responses to other questions confirm this self-evaluation. Considering that 70% of the respondents are enrolled in software engineering and are a respectively young population, and one third do not have much knowledge on cyber security, this lack of knowledge is likely to be much higher in the general population. The difference between male and female and age range is not significant (1-3%) (Chart 1)



Privacy

The respondents were asked to select the information type that they consider to be private. The data that respondents considered most private was bank account information 20%, followed by contact information (17%), pictures (15%), location (15%), and IP address on the device (14%). Again, there were no significant differences between female, male population and groups of age. Overall it seems that with a light advantage on bank information user consider most of the area questions as private information.

The participants were asked to rate how secure their communication platforms were. For this question the respondents were asked to rate the security of each platform on a scale of 1 to 10 (1 being the least secure and 10 being the most secure). In this case what was ranked (Strongly agree and Somewhat agree) higher were: online banking (63%) Mobile Banking (60%), Email (33%), Texting and Mobile Texting (25%) and Social Networking 12% (Chart 2)



On app permission requests, 50% responded that they have rejected the permission (54% females and 49% males), 43% sometimes rejected app permission requests, and only 7% have never rejected the request.

For the question of whether or not respondents had ever rejected a mobile app request for accessing their contacts, camera or location, 45% responded “Yes” (51% females and 43% males, 40% of the 18-24 age group and 52% of the 25-34 age group). The “No” responses were 39% and 16% replied “Not sure”. The younger age group (18-24) reject less app permissions to use contacts (43% “No”) versus the older group (24-34) of which 33% replied “No”. Considering that 39% answered no to the question, “Do you ever reject app permissions?" and 43% said they sometimes rejected app permissions, we might extrapolate that in fact there might be much less people that reject app requests to access their unneeded data on a mobile phone.

Trust

62% of respondents had reason to believe that they were being observed online without their consent, 15% had no reason to believe, and 23% were not sure. This might be an indicator of the trust of Internet privacy.

Trust of University Data Security

For the perception of data security of university systems, only 8% believed that their data was secure (5% females and 10% males) 57% believed that data was relatively secure on university systems (66% female and 53% males), 21% declared not secure (18% females and 25% males), and 13% not sure.

For the last question concerning the Learning Management System, 8% believed it to be secure, 43% relatively secure, 18% not secure, and 31% not sure.

Password

In terms of password selection, the participants were asked if they use a harder-to-guess password to access their bank account than to access their social networking accounts. 53% declared that they use a harder-to-guess password for their bank account than for social networking. 17% used the same complexity for both passwords and 30% said they use different passwords but the same complexity for both. In this case the difference between females and males is 5% and difference between the two age groups (18-24 and 25-34) is 7% for "No, use the same for both". However, for "No, use different for each but similar level of complexity" the difference between females and males is 3% and between age groups is 10%.

52% of respondents (59% females and 49% males and 40% of 18-24 and 55% of 25-34 age groups) use two factor authentications for some accounts and 24% (13% females and 30% male) use for all accounts.

4 Data Analysis

In this section the data in the above questions are analyzed.

Knowledge of Cyber Security

60% of respondents agreed that they are knowledgeable of cyber security. This can be considered a good percentage. However, the 40% who do not have knowledge of cyber security is significant especially since most are younger college students assumed to have greater knowledge of computers. It is also important to underline the considerable percentage (16%) of participants who recognize not having any knowledge of cyber security. Considering that this is a self-evaluation question, we can conclude that the people who claim to be knowledgeable might not necessary apply their knowledge for better security. However, this degree of awareness is much better than employees. Mediapro surveyed more than 1,000 employees across the U.S. seven out of ten employees lack the awareness to stop preventable cyber security incidents[11].

This survey does not support the assumption that the people with a higher level of cyber security knowledge will be more careful in their cyber security and will try to secure themselves. For example, data indicates that among the people who consider

themselves knowledgeable, only 52% use two factor authentication for some accounts or they do not have a secure password for all their accounts, and that a surprising 8% do not even know what two-factor authentication is.

Security awareness is considered the first line of defense for the security of information and network. [12] Consequently, incorporating training to improve security awareness among college students, and even earlier at the high school level, seems to be extremely important.

Password

Password security still remains one of the main issues in authentication. This includes the complexity of passwords and two-factor authentications. 53% of respondents declare they have a harder-to-guess password for their bank account than social networking accounts. 30% of respondents use the same complexity for both types.

While one might consider that a hard-to-guess password is only essential for sites that store private information, an easy to hack social networking account can open the door for a lot of social engineering or ransom attacks. Therefore, a hard-to-guess password is needed for all types of accounts that include user data.

This issue also indicates that 52% of respondents use two-factor authentication for some accounts and 24% use it for all accounts. 3% don't use it at all and 8% do not know even what it is. Considering that the respondents are university students, this seems to be a very alarming issue.

It seems that among college students, adopting and using better security practices still needs to be improved.

Privacy

The same type of issue is revealed for respondents who consider their bank account, contact information, and pictures as their most private information. In general, respondents considered almost all the above information as private. However, they consider their IP address or locations as less private than their contact information even though we know that most contact information is available on the Internet. In fact, a great deal of contact information can be purchased on the Internet for a few dollars from legal sources while IP addresses and location might be harder to get.

Another parameter that still illustrates low awareness of cyber security among college students is the under usage of two-factor authentication. Only 50% claim that they use it.

While we see a low degree of preventive measures being taken by college students, it is interesting to observe that 63% of respondents have reason to believe that they are being watched online without their consent.

Interestingly when the respondents were asked if they have rejected app permissions, 50% said “Yes” and 43% said "Sometimes". This might indicate that when it is easy to see which application asked for the users' permission, most of the time the users might make a judgment not to let the application access data they consider to be private. This result confirmed a previous survey [13] that reported that 92% (153 participants) of those surveyed expressed that they “Yes” have rejected access if they believe the app does not need to access the camera or contacts. This result is also in line with a related previous study by Haggerty J., et al (2015) [14] who found that 74.1% of iOS users would reject the app permissions list. However, in many instances users do accept granting permissions requested by the majority of applications and the percentage in this study is much lower than the previous study.

It is also important to underline that despite awareness of importance of Internet privacy, college students are still willing to engage in risky online activities. [15] Consequently, young adults need to be motivated to enact security precautions and they should take seriously the risks of Internet use or online safety communication and consider it as personal responsibility.[16]

Trust

Another important factor in security was the perception of trust in computer systems. The trust perception was evaluated through three questions: Trust of the Internet (Do you have reason to believe that you are being observed online without your consent?) and trust of the university system (“Do you think that your data on the university system is secure?” and “Do you think your communication through Learning Management System is secure?”). Interestingly 62% of respondents (64% females and 62% males and 58% aged 18-24 and 67% aged 25-36) believe they are observed online without their consent. It seems that the percentage goes up with older age groups. It would be interesting to investigate what factors make them believe they are watched online and how. Is it just their search behavior or more?

The trust of security of the university system (including learning management) is not necessarily very high. Only 8% (5% of female respondents and 10% of males) think that the system is secure. However, 57% consider it to be relatively secure. It is also important to underline that 21% believe it is not secure.

5 Conclusion

The results of this survey indicate that college students, despite their belief that they are observed when using the Internet and that their data is not secure even on university systems, still are not very aware of how to protect their data. For example, they reported low levels of two-factor authentication usage or password complexity for accounts. Also, it appears that educational institutions do not have an active approach to improve awareness among college students to increase their knowledge of these issues and how to protect themselves from potential cyber-attacks, such as identity

theft or ransomware. It is also reported that most students are aware of possible consequences of providing personally identifiable information to an entire university population, such as identity theft and stalking, but nevertheless feel comfortable providing it. [16]

References

[1] White Gillian N. (2017) A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable. Sept. 7, 2017, The Atlantic.
https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/

[2] Cuthbertson A. (2017) Ransomware Attacks rise 250 percent in 2017, Hitting U.S. Hardest. Sept. 28, 2017, Newsweek.
http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034

[3] Reyns W.B. (2010) Stalking in the Twilight Zone: Extent of Cyberstalking Victimization. Journal Deviant Behavior, Volume 33, 2012 - Issue 1.
http://www.tandfonline.com/doi/abs/10.1080/01639625.2010.538364

[4] Farzan A. (2015) College students are not as worried as they should be about the threat of identity theft. June 9, 2015, Business Insider.
http://www.businessinsider.com/students-identity-theft-2015-6

[5] Dakss B. (2007) College Students Prime Target for ID Theft. August 21, 2007, CBS News.
https://www.cbsnews.com/news/college-students-prime-target-for-id-theft/

[6] Slusky L. and Partow-Navid P. (2014) Students Information Security Practices and Awareness. Journal of Information Privacy and Security, Pages 3-26. Published online July 7, 2014.
http://www.tandfonline.com/doi/abs/10.1080/15536548.2012.10845664

[7] Samaher Al-Janabi and Ibrahim Al-Shourbaji (2016) A Study of Cyber Security Awareness in Educational Environment in the Middle East. Info. Know. Mgmt. 15, 1650007 30 pages.
https://doi.org/10.1142/S0219649216500076

[8] Senthilkumar K. and Easwaramoorthy s. (2017): A Survey on Cyber Security awareness among college students in Tamil Nadu, IOP Conference Series: Materials Science and Engineering, Volume 263, Computation and Information Technology

[9] Grainne H. et al. (2017) : Factors for Social Networking Site Scam Victimization Among Malaysian Students, Cyberpsychology, Behavior, and Social Networking, October 2017.
https://doi.org/10.1089/cyber.2016.0714

[10] SJSU, Institutional Effectiveness and Analytics, Access November 107
http://www.iea.sjsu.edu/Students/QuickFacts/default.cfm?version=graphic

[11] Schwartz J. (2017): Report: 7 in 10 Employees Struggle with Cyber Awareness,
https://www.mediapro.com/blog/2017-state-privacy-security-awareness-report/

[12] OECD (2002): OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, European Union Agency for Network and Information Security, July 25, 20012.
https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/corporate-governance/oecd-guidelines

[13] Moallem A. (2017): Do You Really Trust "Privacy Policy" or "Terms of Use" Agreements Without Reading Them?, springe, Advances in Human Factors in Cybersecurity pp 290-295

[14] Haggerty J., et al (2015), Hobson's choice: Security and Privacy Permissions in Android and iOS Devices. IN t. Tryfonas and I. Askoxylakis (Eds.), Springer International Publishing Switzerland, (2015).

[15] Govani T. and Pashley H. (2009) Student Awareness of the Privacy Implications When Using Facebook.
http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

[16] Jan Boehmer J. et al. (2014) Determinants of online safety behaviour: towards an intervention strategy for college students. Journal Behaviour & Information Technology, Volume 34, 2015 - Issue 10 Pages 1022-1035.
https://scholars.opb.msu.edu/en/publications/determinants-of-online-safety-behaviour-towards-an-intervention-s-3